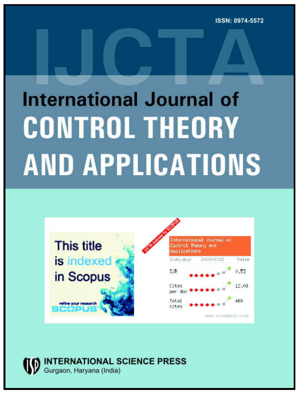


ISSN: 0974-5572

IJCTA

International Journal of
CONTROL THEORY
AND APPLICATIONS

This title is indexed in Scopus

INTERNATIONAL SCIENCE PRESS
Gurgaon, Haryana (India)

International Journal of Control Theory and Applications

ISSN : 0974-5572

© International Science Press

Volume 10 • Number 15 • 2017

Novel Arnold Scrambling Based CBC-AES Image Encryption

Vinita Shadangi[1], Siddharth Kumar Choudhary[1], K. Abhimanyu Kumar Patro[1] and Bibhudendra Acharya[1]

[1] Department of Electronics and Telecommunication Engineering National Institute of Technology, Raipur, Chhattisgarh, India,
Emails: vini.shadangi@gmail.com, siddharthc1995@gmail.com, abhimanyu.patro@gmail.com, bacharya.etc@nitrr.ac.in

Abstract: The security of digital images has become a serious issue now-a-days, especially when the images are sent through a communication network. For secure communication, there are innumerable ways of encryption and decryption of digital images. In this paper, a novel Arnold scrambling based CBC-AES image encryption algorithm is proposed which have multiple levels of encryption. Because of multiple levels of encryption, it is not possible for the eavesdropper to recover the original image. In this algorithm, initially, the input image is circularly shifted and Arnold scrambled along with bitwise shuffle operation, after that each bit is complemented. Finally CBC mode of AES encryption scheme has been applied to obtain the resultant cipher image. From the simulation results, found that the proposed algorithm is effective for encryption of digital images. The security analysis shows that this algorithm has the ability of resisting several attacks such as statistical attack, differential attack and entropy attack.

Keywords: Image Encryption, Arnold Scrambling, CBC (Cipher Block Chaining) Mode, AES (Advanced Encryption Standard) Method.

1. INTRODUCTION

With the rapid advancement of internet and network technology, the security of digital images has become an issue during transmission over an open network. Thus to protect digital images against unauthorized access, various image encryption techniques, such as DES [1], 3DES, AES [2], etc. are used before being transmitted over an open network [3 – 5]. However, due to some special features of digital images such as huge data capacity, high redundancy and strong correlation among adjacent pixels, these traditional image encryption techniques are not very much suitable for image encryption [6, 7].

For better image encryption, many researchers developed different image encryption techniques along with traditional image encryption techniques. In 2000, Dang et al. [3] proposed a joint image compression and encryption technique where Discrete Wavelet Transform (DWT) is used for performing compression and DES is used for performing encryption. Since DES requires more computations for processing large amounts of data so to overcome this problem, researchers used AES based techniques for processing large amounts of digital data

[4]. In 2007, Zeghid et al. [4] proposed a modified AES based image encryption algorithm where a key stream generator is used with AES to modify the AES algorithm. This scheme not only improves the encryption performance but also increases the security. The textured zone problem which was there in other encryption techniques are solved by using this technique. In [8], a modified AES proposed for securing digital images. The modification is done in terms of row shift transformation. In this paper we use AES based image encryption technique to encrypt digital images.

There are basically five standard modes of operation that are used with block cipher to encrypt large amounts of the digital data. Out of the five standard modes of operation, Electronic Code Book (ECB) mode is the most apparent one. But block ciphers operated in ECB mode is not secure for a large size message because for a large size message the same plain text block is repeated many times. In ECB mode, the same block of plain text data will give the same block of cipher text data. So this is the main security issue in ECB mode [4]. In this paper, we use Cipher Block Chaining (CBC) mode of operation with AES algorithm which provide improved security than the ECB mode and also more appropriate for communicating large amounts of digital data [18]. In this mode of operation, the same block of plain text data will not give the same block of cipher text data, so it is secure one as compared to the ECB mode.

For better image encryption, in this paper, we use one of the most famous scrambling techniques, Arnold cat map [9 – 12] and it is combined with AES to scramble the pixels in the original image. This gives higher security than AES alone when used for encryption. In this paper, proposed encryption technique have various stages, such as, first circular shifting, second scrambling, third bit-wise shuffling, and at last CBC mode of operation based AES to get final ciphered output.

The remaining of this paper is organized in the following way. Section 2 summarizes about Arnold Scrambling, AES, and CBC mode of operation. In section 3 proposed methodology described. The simulation results and security analysis are presented in Section 4. Finally, this paper is concluded in Section 5.

2. PRELIMINARIES

In this section, the Arnold scrambling, AES, and CBC mode of operation are outlined.

2.1. Arnold Scrambling

Scrambling is an important concept in image encryption. So, according to the concept of scrambling transformation, the pixel position of the original image is altered from the original pixel position. The 'degree of scrambling' depends on the distance between the two pixel positions such as original pixel position and the new pixel position. Larger the distance higher is the degree of scrambling. In scrambling, the pixel gray values are not changed, only the pixel positions are changed. Due to that, the original contents of an image shown to be secret and will not be easily intercepted by the interceptor. Arnold scrambling is one of the most popular scrambling technology.

V. I. Arnold, the Mathematician [13], first proposed Arnold transform (also called as cat mapping) in their research of ergodic theory. Since Arnold scrambling algorithm is very much simple and also periodic in nature, hence it is widely used for scrambling operation [14]. The Arnold transform is operated in the following way.

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} 1 & a \\ b & 1+ab \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} (\text{mod} \quad M) \text{ where } a \geq 1 \text{ and } b \geq 1 \tag{1}$$

For the sake of simplicity, the value of a and b is taken to be 1. Here, M denotes the size of the original image which is $M \times M$. (x, y) denote the coordinate of the pixel before applying Arnold transformation and after Arnold transformation, let it will be (x', y').

2.2. The AES Technique

The AES algorithm is a symmetric block cipher algorithm by NIST to overcome the problems in DES [15]. The AES algorithm operated with different key lengths such as 128 – bits, 192 – bits or 256 – bits. With corresponding key lengths, the number of rounds of transformation is also different. That means for 128 – bits key length, the number of rounds are 10, similarly for 192 – bits key length, the number of rounds are 12 and for 256 – bits key length the number of rounds of transformation are 14 [16, 17]. The encryption and decryption block diagram for AES algorithm is shown in Figure 1. The figure shows the number of transformations for each round of encryption. The numbers of transformation operations for each round of encryption except the last round are, Substitute Byte Transformation, Shift Rows Transformation, Mix Columns Transformation and the last one is Add Round Key Transformation. But in the last round Mix Columns Transformation operation is absent. The AES also comprises of Key Expansion and Initial Add Round Key transformation operation.

2.3. Cipher Block Chaining Mode

Out of the five different modes of operation, CBC is one of the superlative methods for encrypting large amounts of the digital data in a secured manner. One of the most important features of CBC mode is that it generates unique blocks of cipher data for the same blocks of input data. So to make unique blocks of cipher data, an initialization vector (IV) of certain length is to be assigned in the first block. It uses a chaining mechanism for encrypting all the blocks of plain text data. The current block of cipher text data depends on the previous block of cipher text data for getting its output. That means if any error or fault occurs in the current cipher text data then it is transmitted succeedingly to the next block of cipher text data. The same thing happens in the decryption also. A single bit error in a ciphertext block of data affects the decryption of all the subsequent blocks of cipher text data. Basically, XOR operation is used for encrypting each block of plaintext data. In this paper, we use AES

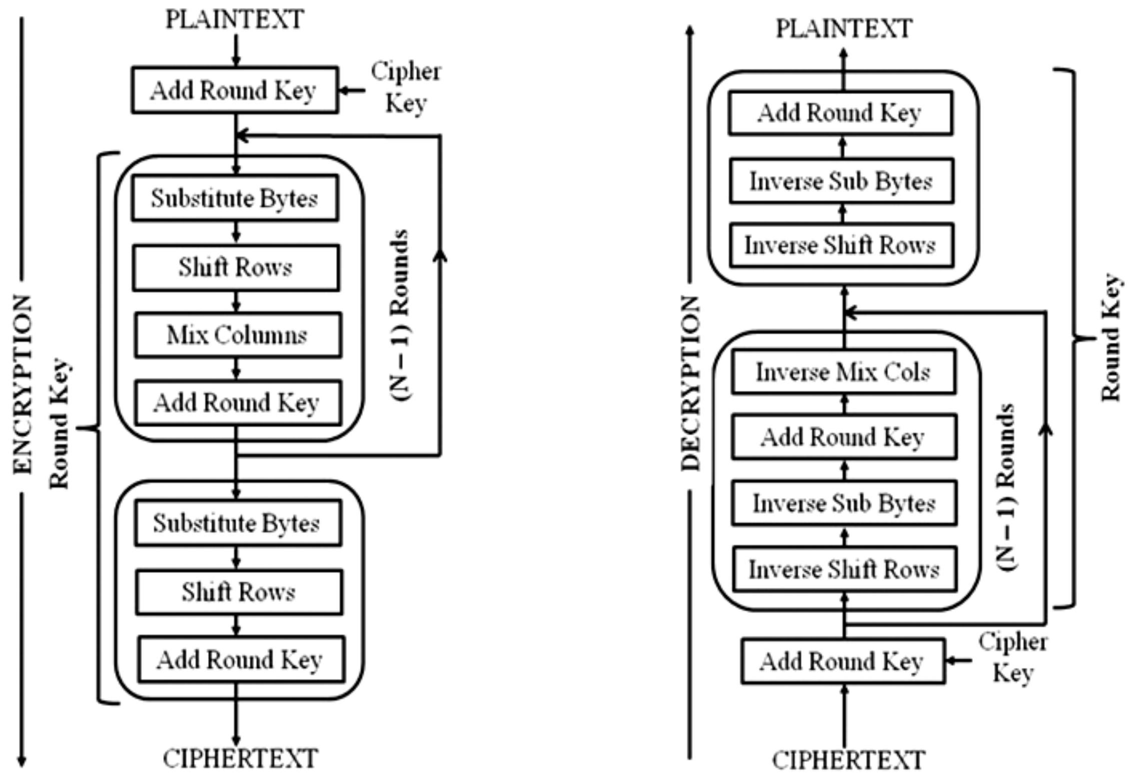


Figure 1: Encryption and decryption block diagram for AES algorithm

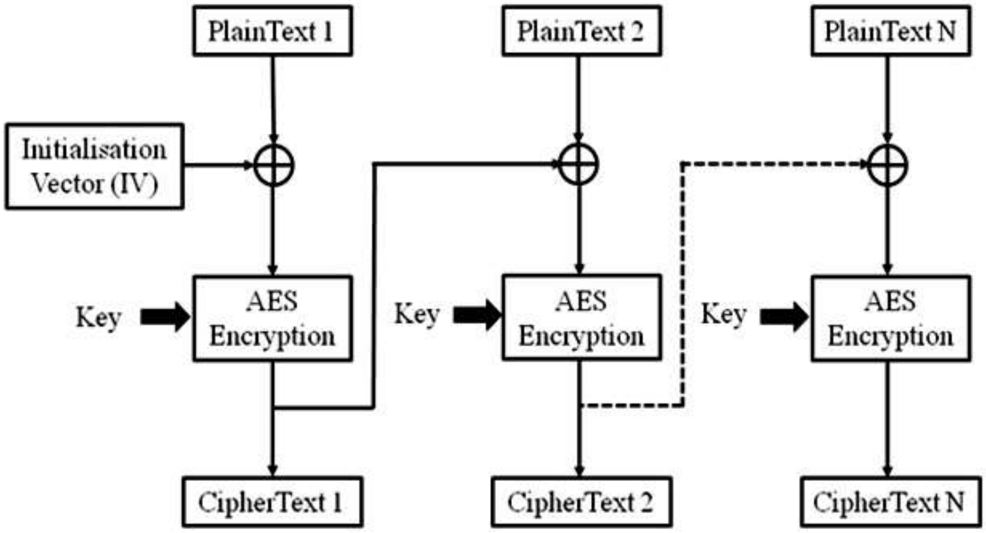


Figure 2: CBC mode of AES encryption

encryption for encrypting each block of plaintext data. The initialization vector need not to be secret, but in some applications it required to be secret. Figure 2 shows the CBC mode of operation using AES encryption.

3. PROPOSED METHODOLOGY

This section presents the proposed image encryption and decryption algorithm. Figure 3 shows the block diagram for image encryption and decryption of the proposed methodology.

3.1. Encryption Algorithm

Step 1: Input the gray-scale image.

Step 2: Perform 100 – times circular left-shift operation to this image.

Step 3: Apply Arnold scrambling to the circular left-shifted image.

Step 4: Perform binary conversion of this rotated image.

Step 5: Perform bit-wise shuffling of each of the pixels in the binarized image and then apply complementation operation to each of the bits of the shuffled binarized image.

Step 6: Finally, apply CBC mode of AES encryption to this complemented image.

Step 7: Store this resultant image as a cipher image.

3.2. Decryption Algorithm

Step 1: Read the ciphered image.

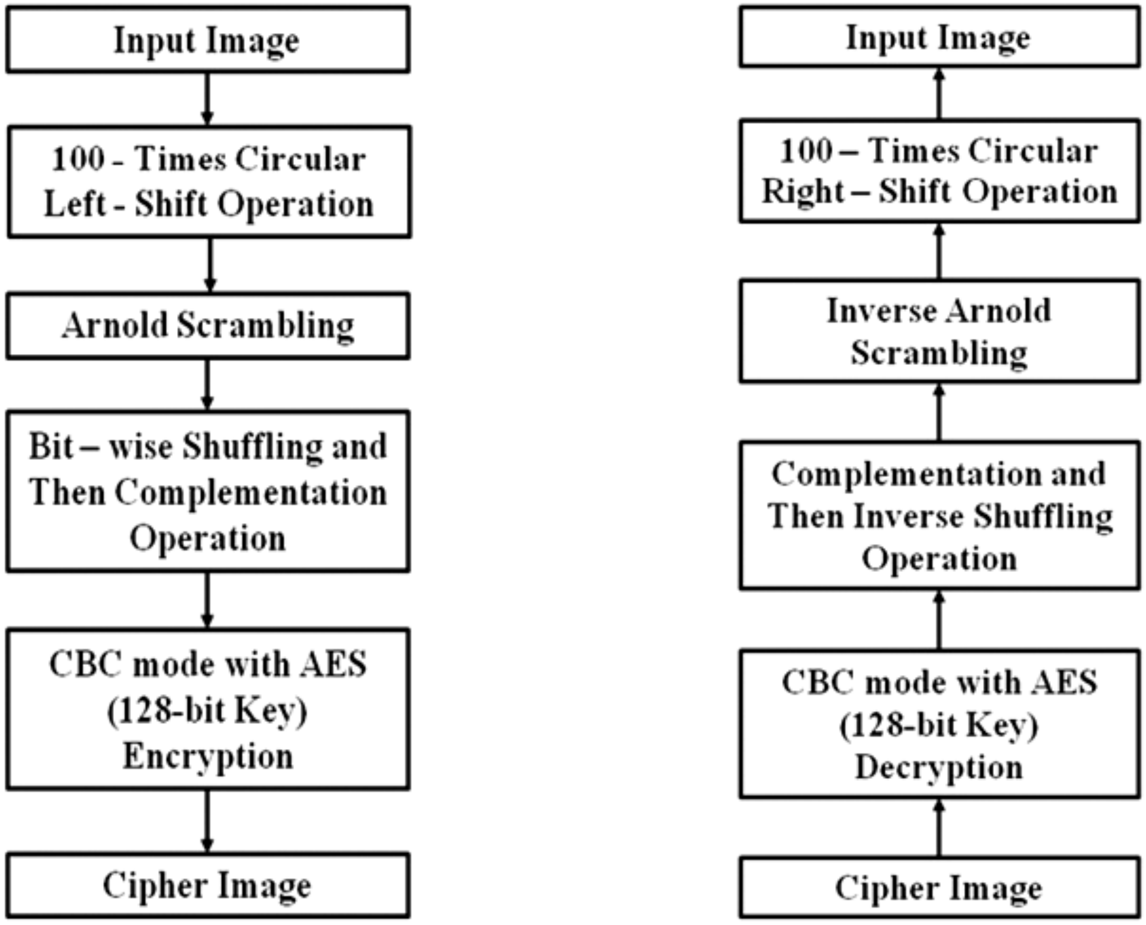
Step 2: Apply CBC mode of AES operation to this cipher image.

Step 3: Perform complementation operation to each of the pixels and then apply inverse shuffling operation to the binary values as like in encryption.

Step 4: Apply inverse Arnold scrambling to this shuffled image.

Step 5: Perform 100-times circular right-shift operation to this scrambled image.

Step 6: Store this resultant image as a decrypted image.


Input Image
100 - Times Circular Left - Shift Operation
Arnold Scrambling
Bit – wise Shuffling and Then Complementation Operation
CBC mode with AES (128-bit Key) Encryption
Cipher Image
Input Image
100 – Times Circular Right – Shift Operation
Inverse Arnold Scrambling
Complementation and Then Inverse Shuffling Operation
CBC mode with AES (128-bit Key) Decryption
Cipher Image

(Encryption) **(Decryption)**

Figure 3: Block diagram of the proposed image encryption and decryption algorithm

4. SIMULATION RESULTS AND SECURITY ANALYSIS

This section presents the simulation results and the security analysis such as key space analysis, statistical analysis, differential analysis, and information entropy analysis of the proposed image encryption and decryption algorithm.

In this research, all images are taken as gray level with dimensions 256 × 256. MATLAB R2012a is used for simulation. The simulation was carried out in a system with windows 8.1 operating system, i5 processor, 1.80 GHz CPU, 8.00 GB memory and 500 GB hard disk. In this the two standard images are used, those are ‘Cameraman’ and ‘Lena’ shown in Figure 4 (a) and (d) respectively. The encrypted results of ‘Cameraman’ and ‘Lena’ are as shown in Figure 4 (b) and (e) respectively. From the two encrypted results, it clearly shows that both the images are properly encrypted by using the proposed algorithm. This means that it is difficult for the hackers to obtain the original information contents from the encrypted image. The decryption results of ‘Cameraman’ and ‘Lena’ are as shown in Figure 4 (c) and (f) respectively. Both the decrypted results show that the encrypted images are properly decrypted by using the proposed algorithm.

The security analyses are as follows.

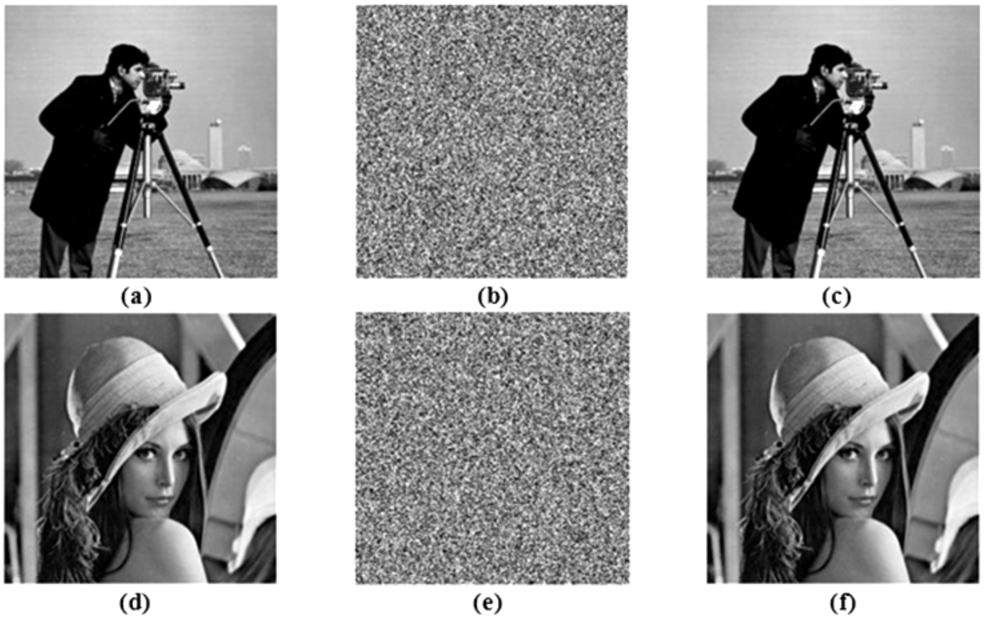


Figure 4: (a) & (d) Original 'Cameraman' and 'Lena' images respectively, (b) & (e) encrypted 'Cameraman' and 'Lena' images respectively by using the proposed algorithm, (c) & (f) decrypted 'Cameraman' and 'Lena' images respectively by using the proposed algorithm

4.1. Key Space Analysis

To provide higher level of security or to make brute-force attack infeasible, the key space should be large enough. But it should not be lesser than 2^{100} [19]. The proposed method uses 128-bit key for AES encryption, two initial conditions and for Arnold scrambling and the initialization vector (if required) for CBC mode of operation. According to the IEEE floating-point standard [20], the computational complexity of a 64 – bit double – precision number is about 10^{15}. So,

$$\text{Total key space} = 10^{128} \times 10^{15} \times 10^{15} \times IV = 10^{158} \times IV$$

which is large enough to resist brute-force attack effectively. So the proposed method is more secure to exhaustive attack. Also the proposed algorithm is sensitive to both key and plaintext.

4.2. Statistical Analysis

An image encryption algorithm is good to use, when it will resist against any statistical attacks [21]. So in order to resist against any statistical attack, certain random properties are to be acquired by the encrypted images. In this paper, we have performed the statistical analysis such as histogram analysis, correlation coefficient analysis to show the robustness of our cryptosystem.

4.2.1. Histogram of Encrypted Image

For generating randomness in the encrypted images, the histogram of encrypted images should be significantly different than the plain images and also it should be uniform in all the grey levels so that the attackers have difficulty for obtaining any useful information [22]. The histogram of original 'Cameraman' image and its corresponding encrypted image by using the proposed cryptosystem are shown in Figure 5 (a) and (b) respectively. Similarly the histogram of standard 'Lena' image and its corresponding encrypted image by using the proposed cryptosystem are shown in Figure 6 (a) and (b) respectively. From the Figures, it is clearly apparent that the

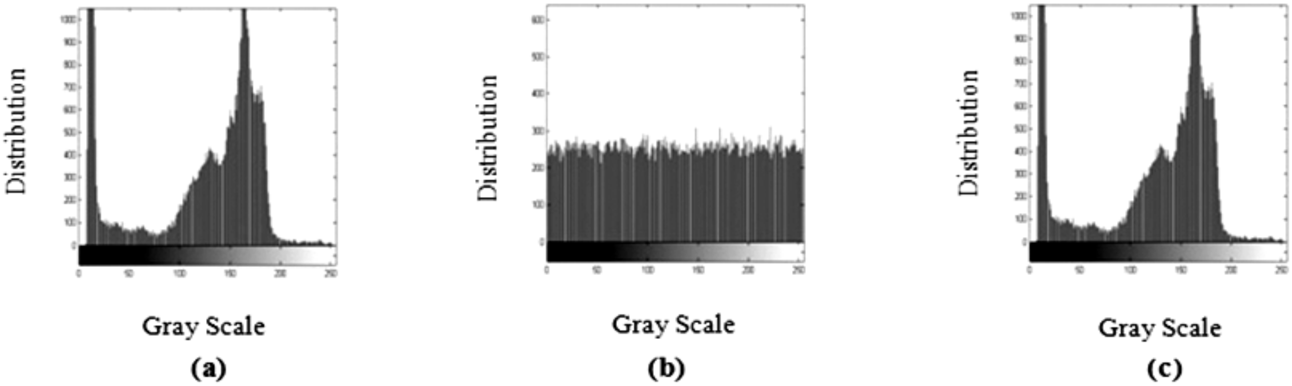


Figure 5: Histograms of 'Cameraman' image: (a) Histogram of original image, (b) Histogram of corresponding encrypted image, (c) Histogram of corresponding decrypted image by using the proposed method.

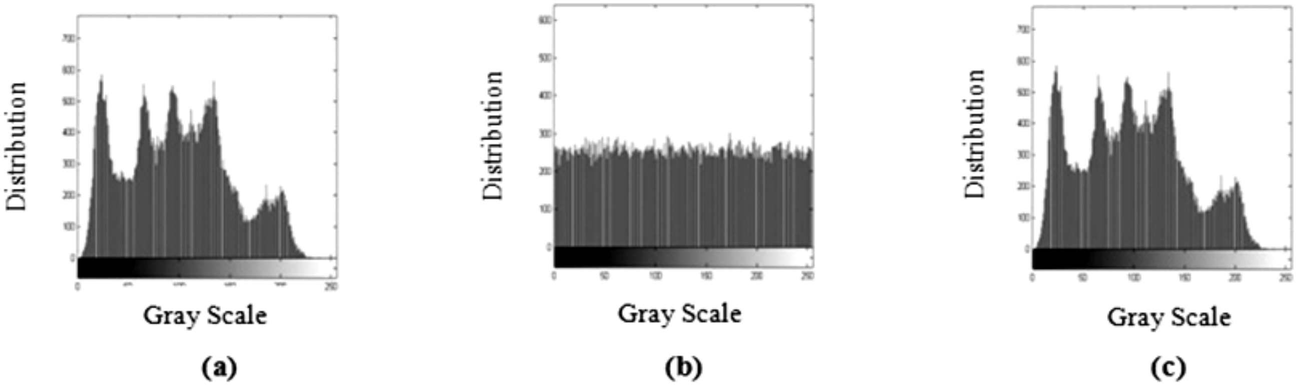


Figure 6: Histograms of 'Lena' image: (a) Histogram of original image, (b) Histogram of corresponding encrypted image, (c) Histogram of corresponding decrypted image by using the proposed method.

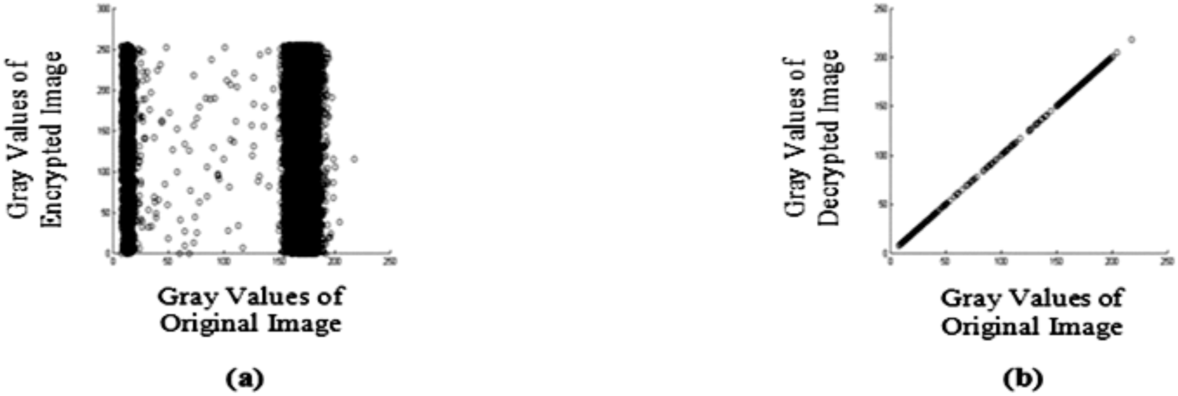


Figure 7: (a) Scattered diagram between original and encrypted images of 'Cameraman' by using the proposed method, (b) Scattered diagram between original and decrypted images of 'Cameraman' by using the proposed method.

histograms of the encrypted images are uniformly distributed and are greatly different than the plain images. Clearly, it is not easy for the hackers to recover the original images by knowing of the encrypted images. Thereby, the proposed method is strong to resist statistical attack. From the histograms of Figure 5 (c) and 6 (c) it shows that there is no loss of data during decryption in the proposed method. So the proposed method is applicable to protect images during communication and transmission. Figure 7 (a) and 8 (a) shows the scattered

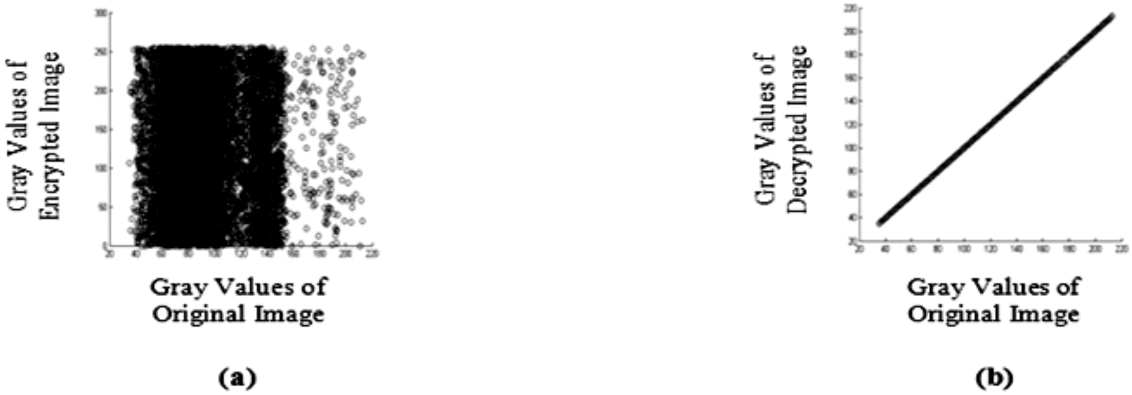


Figure 8: (a) Scattered diagram between original and encrypted images of 'Lena' by using the proposed method, (b) Scattered diagram between original and decrypted images of 'Lena' by using the proposed method.

diagram between original and encrypted images of 'Cameraman' and 'Lena' respectively by using the proposed method. It finds that, the points are not in a line, it spreads throughout the surface. That means weaker correlation occurs between original and encrypted images. Figure 7 (b) and 8 (b) shows the scattered diagram between original and decrypted images of 'Cameraman' and 'Lena' respectively by using the proposed method. It finds that, all the points are along a line. That means stronger correlation occurs between original and decrypted images.

4.2.2. Correlation Coefficient of Adjacent Pixels

Correlation coefficient of adjacent pixels defines how the adjacent pixels are correlated with each other in an image. Basically, in a plain image, the adjacent pixels for all the three directions (horizontal, vertical and diagonal) are highly correlated (approximate to 1) with each other but for an encrypted image, that correlation of adjacent pixels along all the three directions should be as small as possible (approximate to 0) [23, 24]. So to improve the statistical performance of an encrypted image that means to improve the resistivity against statistical attack, the correlation coefficient of encrypted image should be approximated to 0 (zero). It can be calculated by using the following set of equations:

$$r_{xy} = \frac{\operatorname{cov}(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \tag{2}$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}\left(x_i - \frac{1}{N}\sum_{i=1}^{N} x_i\right)^2 \tag{3}$$

$$\operatorname{cov}(x,y) = \frac{1}{N}\sum_{i=1}^{N}\left(x_i - E(x)\right)\left(y_i - E(y)\right) \tag{4}$$

where *x* and *y* are grey scale values of two adjacent pixels in the image and *E* denotes the expectation operator shown in

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i \tag{5}$$

For calculating correlation coefficient between two adjacent pixels, at first, we randomly selected 4096 pairs of adjacent pixels along all the three directions. Then calculated the correlation coefficient between these pairs of adjacent pixels, which are as shown in Table 1. From Table 1, we found that the correlation coefficient of original images are approximate to 1 (strong correlation) while the correlation coefficient of encrypted images by using the proposed method are approximate to 0 (weak correlation) in all the three directions that means no similarity occurs between original images and encrypted images. This proves that the proposed cryptosystem can effectively resist pixel correlation statistical attack. Figure 9 shows the correlation distribution of two adjacent pixels for original 'Cameraman' image whereas Figure 10 shows the correlation distribution of two adjacent pixels for standard 'Lena' image. From these two contrast diagrams we can observe that the original image have very strong linear correlation, while the encrypted image have very small which simply damages the linear correlation of original image. Therefore the proposed cryptosystem is resistive to pixel correlation statistical attack.

Table 1
Comparison of correlation coefficients between AES method and the proposed method

	Plain Images		*Encrypted Images by using AES Method*		*Encrypted Images by using Proposed Method*	
Correlation Coefficient	*Cameraman*	*Lena*	*Cameraman*	*Lena*	*Cameraman*	*Lena*
Horizontal (H)	0.9335	0.9400	-0.0039	-0.0041	-0.0007	0.0050
Vertical (V)	0.9592	0.9693	0.0058	-0.0015	0.0029	-0.0021
Diagonal (D)	0.9087	0.9179	0.0023	0.0004	0.0020	- 0.0002
(H2 + V2 + D2)0.5	1.6178	1.6327	0.0073	0.0044	0.0036	0.0054
Average (H, V, D)	0.9338	0.9424	0.0014	-0.0018	0.0014	0.0009

4.3. Differential Analysis

The challenging task for all the cryptosystem is that the encrypted image should be significantly different to the original one. So to quantify such difference we use NPCR (Number of Pixel Changing Rate), UACI (Unified Average Changing Intensity), and MAE (Mean Absolute Error) in this paper.

NPCR measures the number of pixel differences between the two cipher images. Let, the two cipher images are denoted as C_1 and C_2 whose corresponding plain images are differed by only one pixel. C_1 *(i, j)* and C_2 *(i, j)* be the corresponding grey level pixel values at i^{th} row and j^{th} column of that image. The NPCR is calculated as

$$NPCR = \frac{\sum_{i,j} D(i,j)}{M \times N} \times 100 \tag{6}$$

Where $M \times N$ is the size of the image which defines the total number of pixels in the image and $D(i, j)$ is defined as

$$D(i,j) = \begin{cases} 0 & C_1(i,j) = C_2(i,j) \\ 1 & C_1(i,j) \neq C_2(i,j) \end{cases} \tag{7}$$

The expected that means the ideal value of NPCR is found to be 99.61 %. For better encryption quality, the NPCR value may be larger than the ideal one.

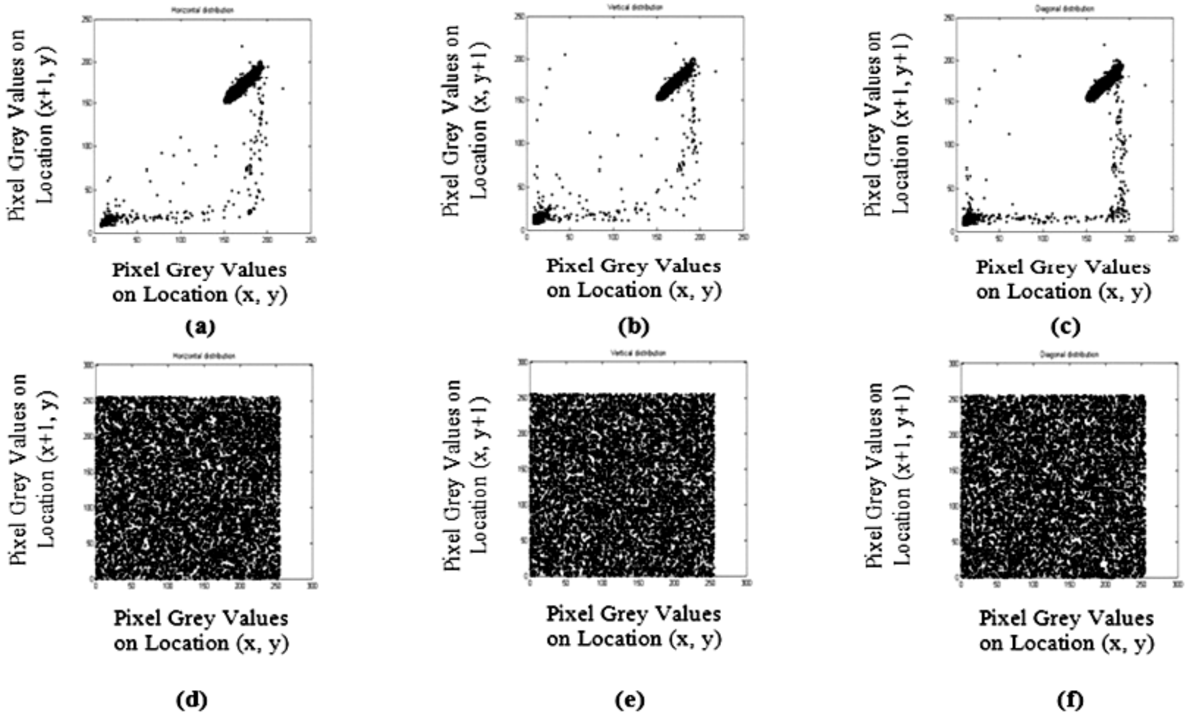


Figure 9: Correlation distribution of two adjacent pixels for 'Cameraman' image: (a, b, c) Horizontal correlation, vertical correlation and diagonal correlation of adjacent pixels of original image, (d, e, f) Horizontal correlation, vertical correlation and diagonal correlation of adjacent pixels of corresponding encrypted image by using the proposed method

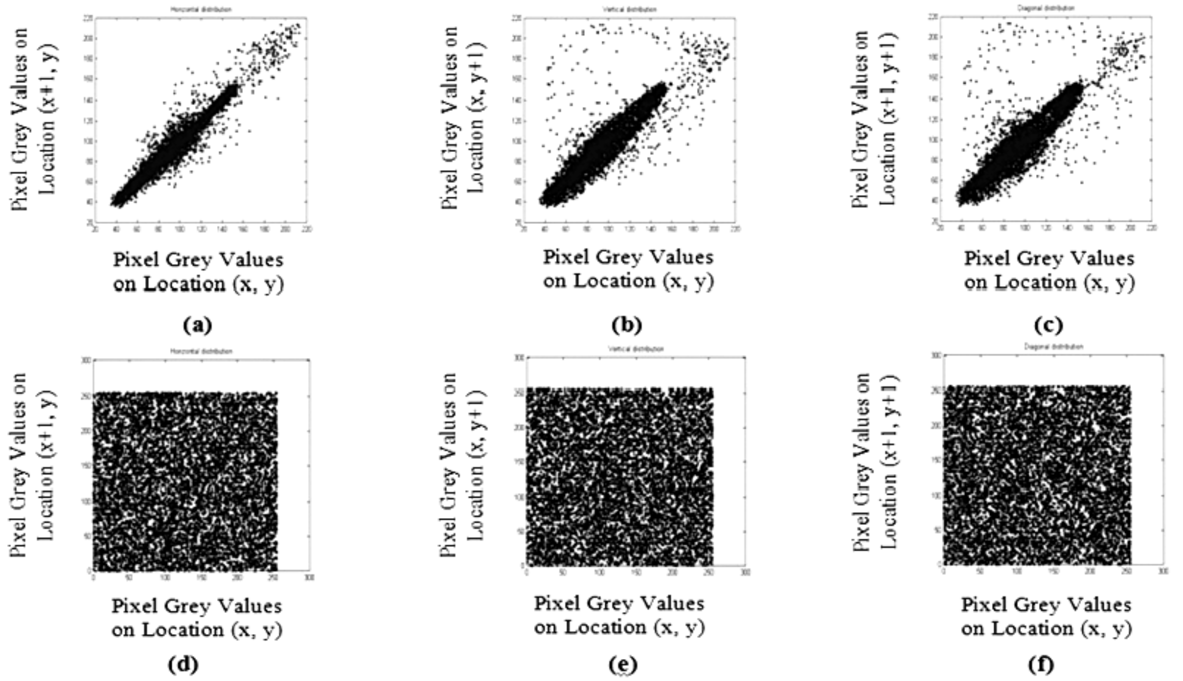


Figure 10: Correlation distribution of two adjacent pixels for 'Lena' image: (a, b, c) Horizontal correlation, vertical correlation and diagonal correlation of adjacent pixels of original image, (d, e, f) Horizontal correlation, vertical correlation and diagonal correlation of adjacent pixels of corresponding encrypted image by using the proposed method

Another measure, UACI, is defined as the average changing intensity between the two cipher images C_1 and C_2. The UACI is calculated as

$$UACI = \frac{1}{N}\left[\sum\nolimits_{i,j} \frac{\left|C_1(i,j) - C_2(i,j)\right|}{2^L - 1}\right] \times 100 \tag{8}$$

In the proposed method, L = 8 – bits, so $2^L - 1 = 255$. The expected that means the ideal value of UACI is found to be 33.46 %. For better encryption quality, the UACI value may be larger than the ideal one.

The MAE between plain image and encrypted image is defined as

$$MAE = \frac{1}{M \times N}\sum_{i=1}^{M}\sum_{j=1}^{N}\left|a_{ij} - b_{ij}\right| \tag{9}$$

where M × N is the size of the images. The parameters a_{ij} and b_{ij} are grey scale values of pixels in original and encrypted images, respectively. The larger the MAE value, the better the encryption security.

The comparison of NPCR, UACI, and MAE criteria of various images by using the proposed method and the AES method is tabulated in Table 2.

Table 2
Comparison of NPCR, UACI, and MAE criteria of the proposed encryption method and the AES encryption method

		Original Image Vs. Encrypted Image	
Criteria (expected value)		*AES Encryption Method*	*Proposed Encryption Method*
NPCR (99.61%)	Cameraman	99.5911	99.6078
	Lena	99.6155	99.6490
UACI (33.46%)	Cameraman	31.0664	31.1380
	Lena	30.5720	30.5237
MAE (Larger Value)	Cameraman	79.2194	79.4020
	Lena	77.9586	77.8354

4.4. Measure of Entropy

Entropy measures the randomness and the unpredictability of an image that may be plain image or an encrypted image. The entropy is calculated as:

$$H_e = -\sum_{k=0}^{G-1} P(k)\log_2\left(P(k)\right) \tag{10}$$

where H_e is the entropy, G is the grey value of the input image, (0....255). *P(k)* is probability of occurrence of symbol *k*. For better encryption quality and for better security of an image, the entropy value of an encrypted image should be approximated to 8. Table 3 presents the entropy of original image and the encrypted image by using both the AES method and the proposed method. A higher value of the entropy obtained in case of our proposed method as compared to that obtained in the AES method indicates that our algorithm introduces more randomness in the encrypted image resulting in better encryption.

Table 3
Entropy of original image and encrypted image by using the AES encryption method and the proposed encryption method

		Encrypted Image	
Images	*Original Image*	*AES Encryption Method*	*Proposed Encryption Method*
Cameraman	7.0097	7.9966	7.9971
Lena	7.5691	7.9974	7.9975

5. CONCLUSION

In this paper, we proposed a novel image encryption technique based on multiple levels of encryptions involving circular shifting, Arnold scrambling, shuffling and finally applying CBC mode using AES. Results of this technique has been analysed and it has been observed that the NPCR, entropy values are improved as compared to the AES method and the UACI value of the proposed methodology is approximately equal to the AES method. Finally, it concluded that the proposed methodology is better than the AES method. With the better encryption of images, it may have application in internet technology such as encryption of images which are transmitted over internet for secure transmission. But the limitation of the proposed algorithm is that it is suitable for encrypting gray-scale images.

The future directions of the proposed approach are as follows:

- This encryption algorithm can be applied to color images by separating out the R (Red), G (Green), and B (Blue) components of the color images.
- In place of Arnold's cat map, we can use hyper-chaotic map for scrambling the pixels of the image.
- We can use SHA – 2 and SHA – 3 algorithms for generating the keys of AES encryption method and for updating the initial values of the Arnold's cat map.

ACKNOWLEDGEMENT

This research work is supported by Information Security Education Awareness (ISEA) project phase – II, Department of Electronics and Information Technology (DeitY), Govt. of India.

REFERENCES

[1] Standard DE. Federal Information Processing Standards Publication 46. National Bureau of Standards, US Department of Commerce. 1977 Jan 15.

[2] FIPS P. 197 FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION. ADVANCED ENCRYPTION STANDARD (AES), National Institute of Standards and Technology. 2001.

[3] P. P. Dang, P. M. Chau, "Image encryption for secure internet multimedia applications", IEEE Transactions on Consumer Electronics, vol. 46, no. 3, pp. 395-403, 2000.

[4] M. Zeghid, M. Machhout, L. Khriji, A. Baganne, R. Tourki, "A modified AES based algorithm for image encryption", International Journal of Computer Science and Engineering, vol. 1, no. 1, pp. 70-75, 2007.

[5] K. Kazlauskas, J. Kazlauskas, "Key-dependent S-box generation in AES block cipher system", Informatica, vol. 20, no. 1, pp. 23-34, 2009.

[6] S. Li, G. Chen, A. Cheung, B. Bhargava, K. T. Lo, "On the design of perceptual MPEG-video encryption algorithms", IEEE Transactions on Circuits and Systems for Video Technology, vol. 17, no. 2, pp. 214-223, 2007.

[7] C. C. Chang, M. S. Hwang, T. S. Chen, "A new encryption algorithm for image cryptosystems", Journal of Systems and Software, vol. 58, no. 2, pp. 83-91, 2001.

[8] S. H. Kamali, R. Shakerian, M. Hedayati, M. Rahmani, “A new modified version of advanced encryption standard based algorithm for image encryption”, International Conference on Electronics and Information Engineering (ICEIE), 2010, Vol. 1, pp. V1-141, 2010, IEEE.

[9] W. Ding, D. X. Qi, “Digital image transformation and information hiding and disguising technology”, Chinese Journal of Computers-Chinese Edition, no. 9, pp. 838-843, 1998.

[10] D. Qi, W. Ding, “A new image transformation scheme and digital approximation between different pictures”, Advances in Computational Mathematics, pp. 202-465, 1998.

[11] Q. Dongxu, “Matrix Transformation and its Applications to Image Hiding”, Journal of North China University of Technology, vol. 1, 1999.

[12] D. Qi, J. Zou, X. Han, “A new class of scrambling transformation and its application in the image information covering”, Science in China Series E: Technological Sciences, vol. 43, no. 3, pp. 304-312.

[13] V. I. Arnol¹d, A. Avez, Ergodic problems of classical mechanics. Benjamin; 1968.

[14] M. Li, T. Liang, Y. J. He, “Arnold transform based image scrambling method”, In International Conference on Multimedia Technology (ICMT 2013), pp. 1309-1316, 2013.

[15] Pub NF. 197: Advanced encryption standard (AES). Federal Information Processing Standards Publication. 2001 Nov 26;197:441-0311.

[16] A. Abdulgader, M. Ismail, N. Zainal, T. Idbeaa, K. S. Yoyon, E. P. Vincentius, O. Benammar, H. Elasri, M. Jebbar, A. Sekkaki, E. Azimirad, “Enhancement of AES algorithm based on chaotic maps and shift operation for image encryption”, Journal of Theoretical and Applied Information Technology, vol. 71, no. 1, pp. 2005-2015, 2015.

[17] W. Stallings, “The advanced encryption standard”, Cryptologia, vol. 26, no. 3, pp. 165-188, 2002.

[18] P. Praveenkumar, G. U. Priyanga, P. Rajalakshmi, K. Thenmozhi, J. B. Rayappan, R. Amirtharajan, ‘2ð rotated Key2 shuffling and scrambling-a cryptic track”, International Conference in Computer Communication and Informatics (ICCCI), pp. 1-4, 2015, IEEE.

[19] D. R. Stinson, Cryptography: Theory and Practice. CRC Press, Boca Raton; 2007.

[20] IEEE Computer Society, IEEE standard for binary floating-point arithmetic. ANSI/IEEE std. 1985;754–1985.

[21] I. Shatheesh Sam, P. Devaraj, R. S. Bhuvaneswaran, “An intertwining chaotic maps based image encryption scheme”, Nonlinear Dyn., vol. 69, pp. 1995–2007, 2012.

[22] J. X. Chen, Z. L. Zhu, C. Fu, H. Yu, L. B. Zhang, “A fast chaos-based image encryption scheme with a dynamic state variables selection mechanism”, Communications in Nonlinear Science and Numerical Simulation, vol. 20, no. 3, pp. 846-860, 2015.

[23] A. N. Pisarchik, M. Zanin, “Image encryption with chaotically coupled chaotic maps”, Physica D: Nonlinear Phenomena, vol. 237, no. 20, pp. 2638-2648, 2008.

[24] S. E. Borujeni, M. Eshghi, “Design and simulation of encryption system based on PRNG and Tompkins-Paige permutation algorithm using VHDL”, In Proceedings of the International Conference on Robotics, Vision, Information and Signal Processing, pp. 63-67, 2007.